View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号____密级___
学号：X2008221001　　UDC____

厦门大学

工 程 硕 士 学 位 论 文

厦门技师学院校园网网络安全设计与实施

The Security Design and Implementation of the Campus Network for Xiamen Technical College

蔡加柳

指导教师姓名：雷蕴奇教授
专　业　名　称：计算机技术
论文提交日期：2012 年　月
论文答辩时间：2012 年　月
学位授予日期：2012 年　月

答辩委员会主席：_____

评　　阅　　人：_____

2012 年　月

厦门大学博硕士论文摘要库

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

摘　要

近几年来，随着计算机网络的普及和发展，高校信息化建设也在快速地进行，校园网在各类高校中的作用越来越大，已经成为高校重要的基础设施。

厦门技师学院从 2007 年搬迁到新校区开始就把校园的信息化建设作为一个重点项目。本文主要根据学院校园网网络安全问题的需求，基于校园网存在的安全隐患和面临的各种安全威胁，针对校园网的安全系统的建设目标，提出了网络系统的安全体系的规划。主要从基础网络的安全设计、第三方的软硬件安全系统、用户认证安全管理系统和无线网络安全等方面进行了设计与实施。根据厦门技师学院现有的网络设备条件采用了 VLAN 技术、防火墙技术、入侵检测防御技术、流量控制、SSL VPN、WLAN 技术以及用户认证安全管理系统实现对校园基本安全防护，保障网络行为的规范性和系统的安全性。该安全体系的架构部署与实施，大大提高了厦门技师学院的校园网的安全系数，不仅保证了校内安全信息资产和网络组件的安全，同时也规范了广大师生的网络行为。无线技术和 VPN 技术的使用也增加了广大师生使用网络资源的灵活性，实现了教师的移动办公和校园内部网的远程接入。

论文还对整个方案中的关键技术进行了大量的数据观测，根据得到的数据网络管理员在技术上和人员管理上都做了相应的策略，保证用户能够安全稳定的接入到网络。篇末还对全文进行了总结，提出了校园网络安全中技术部分存在的问题，对网络安全技术的发展进行了展望，并给出了将来需要进一步研究的方向。

关键字：VLAN；入侵检测；VPN

厦门大学博硕士论文摘要库

Abstract

In recent years with the popularization and development of computer network, the information system of College is developing very quickly, the growing role of the campus network in various colleges and universities has become an important basic establishment in the universities.

Xiamen Technical College put the campus construction as a key project when relocating to the new campus from 2007. This article mainly bases on the requirement of security for campus network, the potential security risks and various security threats to meet the goal of building of the campus network security system, raise the plan for security system of network which are separately designed and implemented from safety of basic network, security system of the third-party's software & hardware, management system for user authentication and wireless network security design. According to Xiamen Technical College of existing network equipment conditions, we use VLAN technology, firewall technology, intrusion detection & prevention technology, flow control, the SSL VPN, WLAN technology and user authentication security management system to achieve the protection on campus security and ensure the network behavior are normative. The deployment and implementation of this security system greatly improves the safety factor of campus network of Xiamen Technical College which is not only to ensure the safety of its information assets and network components, but also standardize the teachers and students' network behavior. Wireless technology and usage of VPN technology has also increase the flexibility of the teachers and students to use network resources, which realize students and teachers' mobile office and remote

厦门大学博硕士论文摘要库

access to the campus intranet.

We did a lot of data observations for the key technology of the whole scheme in the paper, according to the data the network manager develop appropriate strategies in the technical and personnel management that make sure the users can access to the network safely and stably. The summarization at the end of the article not only put forward the partial problem of the existing network security and expect the development of security technology, but also provide the direction of further research in the future.

Keywords: VLAN; Intrusion Detection; VPN

厦门大学博硕士论文摘要库

目 录

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

CONTENTS

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

第一章 绪论

1.1 概述

1.1.1 网络安全的现状

随着信息化进程的不断深入和网络的迅速发展，人们的工作、学习和生活越来越依赖网络，并达到了前所未有的程度，但我们在享受网络所带来的便利的同时，也必须看到紧随网络发展而来的网络安全问题。网络安全是一个关系国家安全和主权、社会稳定、民族文化的继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快而变得越来越重要[1]。

现今面临的网络安全问题，无论是技术手段、数量，还是规模、性质，都已到了人们难以估计的程度。据有关方面统计[2]，世界上平均每 20 秒就发生一次网络入侵事件，另外美国每年由于网络安全问题而遭受的经济损失超过 170 亿美元，法国、英国也均在数十亿美元以上，日本、韩国的问题也很严重。在国内，2011 年 6 月 CNCERT 监测数据的监测报告显示[3]境内感染网络病毒的终端数约为 815 万个；境内被篡改网站数量为 3164 个，其中被篡改政府网站数量为 333 个；国家信息安全漏洞共享平台收集整理信息系统安全漏洞 447 个，其中高危漏洞 250 个，可被利用来实施远程攻击的漏洞有 406 个。

1.1.2 网络安全问题的存在

可以从不同角度对网络安全做出不同的解释。一般意义上，网络安全是指信息安全和控制安全两部分。国际标准化组织把信息安全定义为“信息的完整性、可用性、保密性和可靠性”，控制安全则指身份认证、不可否认性、授权和访问控制[4]。

互联网与生俱有的分散性、交互性和开放性特征使人类所憧憬的信息共享、开放、灵活和快速等需求得到满足。网络环境为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用，为人类社会的进步提供了巨

厦门大学博硕士论文摘要库

大推动力。然而，正是由于互联网的上述特性，产生了许多安全问题。

（1）网络应用的发展的趋势是全社会广泛参与，当然随之而来的是控制权分散的管理问题。由于人们利益、目标、价值的分歧，使信息资源的保护和管理出现脱节和真空，从而使信息安全问题变得广泛而复杂。

（2）信息泄漏、信息污染、信息不易受控。比如资源未授权侵用、未授权信息流出现、系统拒绝信息流等，这些都是信息安全的技术难点。

（3）在网络环境中，一些组织或个人出于某种特殊目的，进行信息泄密、信息破坏、信息侵权和意识形态的信息渗透，甚至通过网络进行政治颠覆等活动，使国家利益、社会公共利益和各类主体的合法权益受到威胁。

（4）随着社会重要基础设施的高度信息化，社会的核心控制系统有可能面临恶意攻击而导致损坏和瘫痪，包括金融系统、国防通信设施和政府网站等。

1.1.3 当前网络安全问题存在的主要原因

1.缺乏的核心技术

虽然我国信息化的步伐很快，但在其发展的过程中缺乏自主技术支撑，特别是 CPU 芯片、网络核心设备以及数据库和操作系统等都是使用国外的。我国计算机网络所使用的网管设备和软件基本上从国外引进的，这些因素使我国计算机网络的安全性能大大降低，被认为是易窥视和易打击的网络。由于缺乏自主技术，我国的网络处于被窃听、干扰、监视和欺诈等多种信息安全威胁中，网络安全处于极脆弱的状态。

2.用户的网络安全意识薄弱

随着网络应用的不断丰富，许多人在工作、学习、娱乐等各个方面都离不开网络，但是大多数用户在享受网络带来的便利的同时并没有注意到随之而来的安全问题，用户的安全意识相当薄弱。与此同时网络运营商和企业用户更多的是注重的是网络带来的效应，而对安全领域的投入和管理远远不能满足安全防范的要求。总体上看，网络信息安全处于被动的封堵漏洞状态，没有形成主动防范、积极应对的全民意识，更无法从根本上提高网络监测、防护、响应和抗击能力[5]。近年来，国家和各级职能部门在信息安全方面已做了大量努力，但就范围、影响和效果来讲，迄今所采取的信息安全保护措施和有关计划还不能从根本上解决目

厦门大学博硕士论文摘要库

前的被动局面，整个信息安全系统在迅速反应、快速行动和预警防范等主要方面，缺少方向感、敏感度和应对能力。

3.运行管理机制的缺陷

运行管理是过程管理，是实现全网安全和动态安全的关键。有关信息安全的政策、计划和管理手段等最终都会在运行管理机制上体现出来。就目前的运行管理机制来看，有以下几方面的缺陷和不足。

（1）缺乏到位的安全措施和专业人才。互联网越来越具有复杂性和动态性特点，这同时也是互联网不安全因素的原因所在。然而，广大的网络用户对此缺乏有效的认识，在没有做好妥善的安全防范措施的时候就进行数据操作，结果往往会导致敏感数据暴露，使系统遭受风险。配置不当或版本较低的操作系统、邮件程序和内部网络都存在入侵者可利用的缺陷，如果缺乏周密有效的安全措施，就无法发现和及时查堵安全漏洞。由于互联网通信成本越来越底，一些服务器和各种不同的网络设备不断的更新。在技术应用的扩展的同时，技术的管理也应同步扩展，但从事网络管理的人员却往往并不具备安全管理所需的专业技能。信息安全技术管理方面的人才无论是水平还是数量，都无法适应信息安全形势的需要。

（2）缺少综合性比较强的解决方案。面对复杂的不断变化的互联网世界，大多数用户缺乏综合性的安全管理解决方案，稍有安全意识的用户越来越依赖防火墙，但这些用户也就此产生了虚假的安全感，渐渐丧失警惕。实际上，一次性使用一种方案并不能保证系统一劳永逸，网络安全问题远远不是防毒软件和防火墙能够解决的，也不是大量标准安全产品简单的部署就能解决的。近年来，国外的一些互联网安全产品厂商及时应变，由防病毒软件供应商转变为企业安全解决方案的提供者，他们相继在我国推出多种全面的企业安全解决方案，包括风险评估和漏洞检测、入侵检测、防火墙和虚拟专用网、防病毒和内容过滤的解决方案，以及企业管理解决方案等一整套综合性安全管理解决方案。

（3）网络安全管理制度的不足。很多企事业单位没有从管理制度上建立相应的安全防范机制，在整个运行过程中，缺乏行之有效的安全检查和应对保护制度。不完善的制度滋长了网络管理者和内部人士自身的违法行为。许多网络犯罪行为都是因为内部联网电脑和系统管理制度疏于管理而得逞的。同时，政策法规

厦门大学博硕士论文摘要库

难以适应网络发展的需要，信息立法还存在相当多的空白。很多信息空间正常运作所需的配套法规尚不健全，如个人隐私保护法、数据库保护法、数字媒体法、数字签名认证法、计算机犯罪法以及计算机安全监管法等。

1.2 厦门技师学院校园网

1.2.1 学院面临的网络安全问题

（1）随着学校的网络应用的不断增加、丰富，加深了学校教学对网络的依赖。大量的学生在宿舍上网，在方便了学生获取知识的同时，也产生了一些其他问题，例如大量的 P2P 流媒体的存在，学校的网络出口拥堵已经成为网络应用性能的主要瓶颈，如何保障网络应用和带宽速度两者之间的平衡，是目前需要解决的首要问题。

（2）目前学校出口仅有一台路由器进行路由策略实现，在网关处的安全防御手段几乎空白，迫切需要在学校网络出口处部署安全设备增强网络的安全性。

（3）学校学生无论是在学习方面的需要，还是个人兴趣爱好，上网过程的网络涉及面均比一般用户广，如何监控、规范学生的上网行为，是目前网络管理需要加强的地方。

（4）高校局域网的网络安全风险（病毒、木马、蠕虫、僵尸等）80%均来自于用户上网过程被感染，如何有效屏蔽 Internet 上的不安全网站，也将是我们需要重点考虑的问题。同时，还需最大限度屏蔽不健康网站（成人、黄色、暴力等），还给学生一个干净的上网环境。

（5）近期校园网 ARP 病毒处于高发状态， 具体原因为校园网内有部分机器上网时中了 ARP 病毒，然后在网内广为传播，导致其它不具备防杀此病毒的机器受感染，由此产生恶性循环。中此病毒的症状为有时候无法正常上网，有时候又好了，包括访问网上邻居也是如此，拷贝文件无法完成，出现错误；局域网内的 ARP 包暴增，使用 ARP 查询的时候会发现不正常的 MAC 地址，或者是错误的 MAC 地址对应，还有就是一个 MAC 地址对应多个 IP 的情况也会有出现。ARP 欺骗的存在大大影响了校园网的性能，同时为学校的信息化办公带来了很大的困难。所以采取一套有效的方案解决该问题，是校园网信息化建设面临的重大难题。

厦门大学博硕士论文摘要库

Degree papers are in the “Xiamen University Electronic Theses and Dissertations Database”. Full texts are available in the following ways:
1. If your library is a CALIS member libraries, please log on http://etd.calis.edu.cn/ and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库